УДК 343.98

Д. С. Захаров,
курсант 4-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Д. И. Шнейдерова,
преподаватель кафедры
уголовного процесса и криминалистики
Могилевского института МВД

ВЫЕМКА ПО ДЕЛАМ О ХИЩЕНИЯХ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ: ВОПРОСЫ ТАКТИКИ

Ежегодное увеличение количества хищений, совершаемых с использованием сети Интернет (мошенничества, вымогательства, хищения путем модификации компьютерной информации) и усложнение механизмов их реализации требуют совершенствования методики их расследования и раскрытия, отдельным пунктом которой является тактика проведения следственных действий. Отдельно среди совокупности требуемых к проведению по данной категории дел следственных действий необходимо остановиться на выемке, которая заключается в принудительном изъятии предметов и документов, имеющих значение для уголовного дела, если точно известно, где и у кого они находятся [1, с. 47]. Объектом выемки при расследовании киберхищений чаще всего становятся носители информации (съемные винчестеры, флеш-карты, оптические диски, холодные криптокошельки), которые хранят файлы различного типа (текстовые, графические, фото, видео, системные и т. д.), готовые программы и приложения, а также в целом системные блоки компьютеров или мобильные устройства, дальнейшее исследование которых позволит получить криминалистически значимую информацию (вредоносные программы, наработки по их созданию, сопровождающие работу данных программ файлы системного характера, скриншоты переписок в социальных сетях или мессенджерах, аудиозаписи разговоров между преступником и потерпевшим, электронные письма, текстовые файлы с личными данными потерпевших, истории посещения интернет-ресурсов, текстовые и графические файлы-руководства к созданию определенных программ и т. д.).

Следует помнить, что для проведения выемки необходимо наличие двух условий: фактического и процессуального. Фактическим обстоятельством для принятия решения о проведении выемки являются достоверные данные о том, какой предмет подлежит изъятию, где и у кого он находится, а также какими идентифицирующими частными признаками обладает (например, цвет, марка, модель, серийный номер, в каком количестве подлежит изъятию). Если следователь (лицо, производящее дознание) не обладает надлежащей информацией

об изымаемом предмете (к примеру, знает, что необходимо изъять, у кого, но не знает где находится этот предмет и в каком количестве), то вместо выемки следует проводить обыск или осмотр. Такая же ситуация может сложиться и в случае, когда неизвестны частные признаки предмета, а только родовые (например, следователь знает, что необходимо у определенного лица по месту его жительства изъять флеш-карту в корпусе черного цвета, но никакими иными сведениями о ней не располагает; следовательно, на месте, где будет производиться выемка, может быть обнаружено несколько флеш-карт, одинаковых по внешним признакам, и вопрос о том, какая подлежит изъятию, останется нерешенным в рамках данного следственного действия). Процессуальным основанием является постановление следователя (лица, производящего дознание) о проведении выемки, которое подлежит санкционированию прокурором только в случае, если изъятие необходимо проводить в жилище или ином законном владении граждан и отсутствует их согласие на это.

Алгоритм проведения выемки, являющийся одной из ключевых частей тактики данного следственного действия, включает три последовательных этапа: подготовительный, рабочий и заключительный. Подготовительному этапу отводится особое место, поскольку именно в рамках него можно выявить фактическое основание для проведения выемки источников электронно-цифровых следов по киберхищениям. Начинать подготовку целесообразно с развернутого допроса лица, обладающего информацией о предмете, подлежащем изъятию. При постановке уточняющих вопросов необходимо ориентироваться на специфику расследуемого события и особенности изымаемого предмета, при необходимости проконсультироваться со специалистами в сфере цифровых технологий. Если итоги допроса позволили прийти к выводу, что достаточно данных для производства выемки, то следует продумать время, место, круг участников и необходимые технические средства (что также может подсказать специалист). При определении круга участников целесообразно пригласить специалиста соответствующего профиля (например, для качественного изъятия узла какой-либо системы или сети), а также понятых, в случае если выемка будет проводиться в жилом помещении без согласия собственника.

В рамках рабочего этапа лицу, у которого производится изъятие конкретного предмета, предъявляется постановление о проведении выемки и предлагается добровольно выдать необходимый предмет. Также не следует оставлять без внимания и процессуальную часть проведения выемки, где следователь (лицо, производящее дознание) обязан разъяснить всем участникам следственного действия их права и обязанности, порядок проведения выемки и предупредить об использовании технических средств. В случае если лицо отказывается выдать подлежащий изъятию предмет добровольно, то следователь (лицо,

производящее дознание) осуществляет выемку принудительно, если точно уверен в месте нахождения предмета. На заключительном этапе выемки составляется протокол, и его копия выдается лицу, у которого производилось изъятие.

Таким образом, при определении тактики проведения выемки по делам о хищениях с использованием Глобальной сети необходимо обращать внимание на качественную подготовку к данному следственному действию с целью выявления достаточных оснований его проведения и технического порядка изъятия предметов, который может требовать присутствия соответствующих IT-специалистов.

1. Шкаплеров Ю. П., Данько И. В. Следственные действия : пособие ; М-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». 2-е изд., стер. Могилев : Могилев. ин-т МВД, 2017. 108 с. Вернуться к статье